(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－58066
（P2002－58066A）
(43)公開日　平成14年２月22日(2002.2.22)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ　５Ｋ０６７

審査請求　未請求　請求項の数９　ＯＬ　外国語出願　（全 22 頁）

(21)出願番号　特願2001－219891(P2001－219891)
(22)出願日　平成13年７月19日(2001.7.19)
(31)優先権主張番号　００４４０２２１．０
(32)優先日　平成12年７月31日(2000.7.31)
(33)優先権主張国　欧州特許庁（ＥＰ）

(71)出願人　391030332
アルカテル
フランス国、75008　パリ、リュ・ラ・ボエティ　54
(72)発明者　シリル・ウー
フランス国、エフ－93190・リブリー－ガルガン、リユ・サン・クロード、30
(72)発明者　ビノツド・クマール
フランス国、エフ－75005・パリ、リユ・ポリボー、15
(74)代理人　100062007
弁理士　川口　義雄　（外１名）

最終頁に続く

(54)【発明の名称】　近距離無線アクセスおよび対応するサービス端末用のインタフェースを介してハイブリッド無線端末とサービス端末の間で近距離無線商取引を行う方法

(57)【要約】
【課題】　ハイブリッド無線端末とサービス端末の間で近距離無線商取引を実行する方法を提供すること。
【解決手段】　ハイブリッド無線端末は、第１インタフェースを介して無線通信ネットワークと、かつ近距離無線アクセス用の第２インタフェースを介してサービス端末と通信可能であるとともに、無線通信ネットワーク内のユーザを認証するためのユーザ認証情報を備える。本発明による方法は、近距離無線用の第２インタフェースを介して少なくともユーザ認証情報を含むメッセージをサービス端末に伝送し、受信したユーザ認証情報を、認証データベースと照合してサービス端末のユーザを認証し、ユーザ認証が正常に終了した場合には、商取引を可能にする。

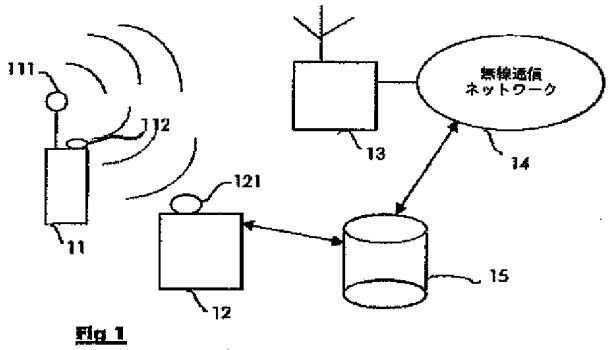

Fig 1

1

【特許請求の範囲】

【請求項１】　ハイブリッド無線端末（１１、３０）とサービス端末（１２）の間で近距離無線商取引を行う方法であって、前記ハイブリッド無線端末（１１）が、第１のインタフェース（１１１）を介して無線通信ネットワーク（１４）と、かつ近距離無線アクセス用の第２のインタフェース（１１２）を介して前記サービス端末（１２）と通信可能であるとともに、前記無線通信ネットワーク（１４）内のユーザを認証するためのユーザ認証情報を備える方法であって、

前記第２インタフェース（１１２）を介して前記ユーザ認証情報を備える前記サービス端末（１２）にメッセージを伝送するステップと、

前記受信ユーザ認証情報を認証データベース（１５）と照合して前記サービス端末（１２）の前記ユーザを認証するステップと、

前記ユーザ認証が正常に終了した場合には前記商取引を可能にするステップとを含む方法。

【請求項２】　前記サービス端末（１２）と前記無線通信ネットワーク（１４）が前記認証データベース（１５）を共有していることを特徴とする請求項１に記載の方法。

【請求項３】　前記認証データベース（１５）が前記無線通信ネットワーク（１４）のホームロケーションレジスタ（ＨＬＲ）であることを特徴とする請求項２に記載の方法。

【請求項４】　前記ハイブリッド無線端末（１１）および前記サービス端末（１２）の近距離アクセス用の前記インタフェースがブルートゥース標準に適合していることを特徴とする請求項１から３のいずれか一項に記載の方法。

【請求項５】　前記ユーザ認証情報がＳＩＭ（加入者識別モジュール）カードの一部であることを特徴とする請求項１から４のいずれか一項に記載の方法。

【請求項６】　近距離無線インタフェース（４１）を介して商取引を実行するための専用のサービス端末（４０）であって、

無線通信ネットワーク内のユーザの認証に専用に用いられているユーザ認証情報を無線端末から受信する手段（４２、４３）と、

前記受信ユーザ認証情報を前記無線通信ネットワークの認証データベース（４５）と照合して前記サービス端末（４０）の前記ユーザを認証するための認証モジュール（４４）とを備え、前記認証が正常に終了した場合には、前記認証モジュールが前記商取引を可能にするサービス端末。

【請求項７】　前記受信ユーザ認証情報を、事前定義された暗号解読アルゴリズムに従って暗号解読するための暗号解読手段をさらに備えることを特徴とする請求項６に記載のサービス端末（４０）。

2

【請求項８】　無線通信ネットワークと通信するための第１パート（３１）と近距離無線インタフェース（３２１）を介してサービス端末と通信するための第２パート（３２）とを備える無線端末（１１、３０）であって、前記第１パート（３１）が前記無線通信ネットワークのユーザを認証するためのユーザ認証モジュール（３１４）を備え、前記第２パート（３２）が前記ユーザ認証モジュール（３１４）へのアクセス権を有すると共に、前記サービス端末の前記ユーザを認証するために、前記近距離無線アクセスインタフェース（３２１）を介して前記サービス端末に少なくとも前記ユーザ認証モジュール（３１４）に包含されているユーザ認証情報を伝送することを特徴とする無線端末（３０）。

【請求項９】　前記ユーザ認証情報を、前記近距離無線インタフェースを介して伝送する前に、事前定義された暗号化アルゴリズムに従って前記ユーザ認証情報の暗号化をさらに行うことを特徴とする請求項８に記載の無線端末（１１、３０）。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は近距離無線データ通信システムに関し、より詳細にはハイブリッド無線端末とサービス端末との間で近距離無線商取引を行う方法に関する。

【０００２】

【従来の技術】ハイブリッド無線端末とは、例えばＧＳＭ移動電話や第３世代ＵＭＴＳ移動電話のような無線通信ネットワークへのアクセス専用であるとともに、例えばブルートゥースインタフェースのような近距離無線アクセス用のインタフェースをさらに備える、無線端末であるといえる。このようなハイブリッド無線端末の例は、ブルートゥース仕様書バージョン１．０Ｂの１００ページに１９９９年１２月１日より知られており、ブルートゥース技術内蔵の「スリー・イン・ワン電話（３－ｉｎ－１　ｐｈｏｎｅ）」モデルが記述されている。

【０００３】家庭では、「スリー・イン・ワン電話」はコードレス電話として機能する。外出中は、セルラー電話として機能する。この最初の二用途については、この移動電話は、無線通信ネットワークに対して通常のインタフェースを使用し、「スリー・イン・ワン電話」は家庭内ではローカル基地局とは例えばＤＥＣＴを介して通信し、外出中はＧＳＭを介して通信する。

【０００４】第３の構成では、「スリー・イン・ワン電話」がブルートゥース技術を内蔵した別の移動電話のレンジ内に入ると、ウォーキートーキーとして機能し、ブルートゥースのインタフェースを介してその別の移動電話と排他的に通信する。この場合には、通信は無線通信ネットワークのリソースを必要としない。さらに、その通信には課金はされない。

【０００５】ブルートゥースは、コンピュータおよび電

気通信の業界仕様であり、移動電話、コンピュータ、パーソナルデジタルアシスタント、およびその他のスタンドアローン型のデバイスを、近距離無線接続を用いて容易に相互接続する方法について記述している。この技術では、それぞれのデバイスに低コストのトランシーバチップを備えることが必要である。各デバイスは、世界的に利用可能な２．４５ＧＨｚ（国によって周波数はいくぶん変動する）の周波数バンドで送受信を行うマイクロチップトランシーバを備える。２つのブルートゥース装備のデバイスを接続できる最大距離は、１０メートルである。ブルートゥースインタフェースを介して、音声通信だけでなくデータ通信もセットアップ可能である。データは毎秒１メガビットの速度で送受信可能である（第２世代技術においては毎秒２メガビットまで）。周波数ホップ方式によって、デバイスは電磁障害が非常に大きな地域でも通信可能になる。各デバイスは、ブルートゥース標準で定義された４８ビットの固有のアドレスによって識別される。この固有アドレスの暗号化および照合の組込み機能が、接続の安全性を保証するために提供されている。しかし、ブルートゥース標準で記述されている照合は、デバイス識別に基づく独自ものである。この識別が原因で、別のブルートゥースデバイスで登録されていないブルートゥースデバイスは相互に通信することができない。このようなデバイスベースの識別の欠点は、ユーザ認証ができないことであり、この結果として近距離無線ブルートゥースのインタフェースを介しては、ユーザ認証を必要とする多くのアプリケーションが不可能である。

【０００６】サービス端末という用語は、このサービス端末を用いて近距離無線インタフェースを介して商取引を開始するユーザに、サービスを提供することのできる端末を取り扱うために用いられる。商取引中に、ユーザはサービス端末で提供されるサービスを要求する。商取引にはサービスを提供する態様の確認とユーザの認証のために、ユーザとサービス端末間の対話が含まれる。認証が正常に終了すると、サービス端末はユーザにサービスを提供して、商取引を終了する。

【０００７】サービス端末によって提供されるサービスは、ユーザに課金されることが好ましいので、サービス端末プロバイダにサービス料金が支払われるのを承認するのにユーザの認証が必要である。このような範疇に入る予想されるサービス端末の例としては、次のようなものがある。料金所で、ゲートが自動的に開くとともに、ブルートゥースインタフェースを備えるハイブリッド移動電話を持つドライバの銀行口座から通行料金を引き落とすサービスや、飲み物自動販売機で、飲み物を買いたいユーザのハイブリッド移動電話から制御して、飲み物の代金を銀行口座から引き落とすか、または電話料金に加算させるサービスなどである。

【０００８】他方で、サービス端末が提供するサービスが秘密のときもある。このような場合には、機密を保持するためにやはりユーザの認証が必要である。この範疇に入るサービス端末の例としては、ハイブリッド移動電話でコントロールされる銀行口座の引出しのプリンタや、ハイブリッド移動電話でコントロールされる医療報告のプリンタがある。

【０００９】

【発明が解決しようとする課題】本発明の特定の目的は、近距離無線インタフェースを介してのユーザ認証の方法を提供し、ハイブリッド移動電話を使ったアプリケーションの範囲を拡大する方法を提供することである。

【００１０】本発明の別の目的は、ハイブリッド端末の機能を利用して、無線通信ネットワーク上のある種のアプリケーションによって生じる負荷を低減することである。

【００１１】

【課題を解決するための手段】前述の目的、および以下に示すその他の目的はハイブリッド無線端末とサービス端末との間で近距離無線商取引を実行する方法によって達成される。ハイブリッド端末は、第１インタフェースを介して無線通信ネットワークと通信可能で、かつ近距離無線アクセス用の第２インタフェースを介してサービス端末と通信可能であるとともに、ハイブリッド無線端末は無線通信ネットワークのユーザを認証するためのユーザ認証情報を備える。その方法とは、近距離無線アクセスの第２インタフェースを介して、サービス端末に少なくともユーザ認証情報を含むメッセージを伝送するステップと、受信したユーザ認証情報と認証データベースとを照合してサービス端末でのユーザを認証するステップと、ユーザ認証が正常に終了した場合に商取引を可能にするステップとを実行することにある。

【００１２】この方法は、ハイブリッド無線端末とサービス端末の間の商取引は、無線通信ネットワークのサービスエリアに依存しないという利点がある。実際に、ユーザが無線通信ネットワークのサービスエリア外にいても、サービス端末と商取引を行うことができる。

【００１３】本方法の別の利点は、サービス端末を用いる商取引が無線通信ネットワークのリソースを何も必要としないために、サービス端末を用いる商取引と無線通信ネットワークを介しての通信が同時に実行できることである。

【００１４】本発明は、請求項６に記載のサービス端末および請求項８に記載のハイブリッド無線端末にも関する。

【００１５】本発明の他の特徴および利点は、制限を加えない実例と添付の図面により示した好ましい実施態様の以下の記述を読むことで明らかになるであろう。

【００１６】

【発明の実施の形態】図１は、本発明による方法を実施することのできるシステムを示している。このシステム

はハイブリッド無線端末１１、無線通信ネットワーク１４に属する基地局１３、サービス端末１２、および認証データベース１５を含む。

【００１７】ハイブリッド無線端末１１は、無線通信ネットワーク１４の基地局１３とエアインタフェースを介して通信するためのアンテナ１１１と、エアインタフェースを介してサービス端末１２と通信するための近距離無線インタフェース１１２を備える。

【００１８】無線通信ネットワーク１４は、ＧＳＭネットワークまたはＵＭＴＳネットワークであるのが好ましい。しかし、認証や承認のような通信セキュリティを保証する機能を提供するその他のいかなる無線通信ネットワークも、無線通信ネットワーク１４の例である。

【００１９】ハイブリッド無線端末１１とサービス端末１２の間の通信に使われる近距離無線インタフェースは、ブルートゥース標準に基づいていることが好ましい。しかし、その他の標準化近距離無線インタフェースも予想される。他の例としては、ホームＲＦ標準がある。ブルートゥースとホームＲＦは両方とも無線周波数通信に基づいている。また、赤外線を用いる光通信も、近距離無線インタフェースを介して使用することができる。赤外線データ協会（ＩｒＤａ）によって策定された標準にそのような赤外線通信が記述されている。

【００２０】近距離無線インタフェースを介しての無線周波数通信の利点は、アンテナを無線通信ネットワーク１４との通信と、サービス端末１２の通信にも使用できることである。近距離無線インタフェースに赤外線通信を用いるには、赤外線放射器をハイブリッド端末に組み込まなくてはならない。

【００２１】近距離無線インタフェースを介しての通信が確立される１つの条件は、ハイブリッド無線端末とサービス端末の間の距離が、標準に示されている無線波を適切に受信するための距離（例えばブルートゥースでは１０メートルまで）に適合していることである。

【００２２】このような距離条件は、無線通信ネットワーク１４との通信については通常、設定されないが、これは無線通信ネットワークのプロバイダの目的は、全エリアがカバーできるようにネットワークを設計することであるからである。これは基地局を適切に配置すること、およびハンドオーバー処理をすることで達成される。反対に近距離無線通信の目標は、互いに近くにあるか、または間に障害物もなく互いに向き合っている２つのデバイス間の通信を可能にすることである。

【００２３】本発明によると、ハイブリッド無線端末１１は、ユーザ認証を実行するために、近距離無線インタフェース１１２を介してサービス端末１２で使用されるユーザ認証情報を伝送する。このユーザ認証情報は、無線端末１１の識別モジュールに配置されており、無線端末１１は、すでに無線端末１１のユーザを無線通信ネットワーク１４内で、認証するために専用化されている。この識別モジュールは、ＳＩＭ（加入者識別モジュール）カードが好ましく、ユーザ認証情報を含むものである。そのようなユーザ認証情報の例としては、ＩＭＳＩまたはＴＭＳＩ（国際適合、臨時移動電話加入者識別）があげられる。他に一義的にユーザを同定できる可能性のあるユーザ認証情報、例えば銀行口座番号または暗証番号もＳＩＭカード上に記憶してもよい。

【００２４】無線通信ネットワーク１４で提供されるセキュリティに匹敵する程度のセキュリティを備える近距離通信を提供するために、サービス端末１２は、サービス端末１２を用いて商取引を行うことを許可されたユーザのユーザ認証情報を包含しているデータベース１５に接続されている。

【００２５】このデータベースは、サービス端末１２に物理的に接続してもよい。またデータベース１５は、サービス端末１２の一部に含まれてもよい。そのような場合には、各サービス端末は、データベース１５の複製版に接続される。

【００２６】代替手法として、このデータベース１５をセンタ要素として、サービス端末１２を適当なネットワークを介して接続してもよい。この構成では、いくつかのサービス端末がデータベース１５に同時に接続される。この場合には、データベースの内容を複製する必要はなく、この結果データの不一致が起こりにくい。

【００２７】好ましい一実施形態においては、データベース１５は、無線通信ネットワーク１４内で認証を行うのに無線通信ネットワーク１４が使うのと同じデータベースである。この実施形態では、データベース１５は、無線通信ネットワーク１４のホームロケーションレジスタ（ＨＬＲ）と対応させてもよい。サービス端末１２は、無線通信ネットワークのオペレータから、セキュリティを確保された特定の接続を介してＨＬＲへのアクセスを許可されている。サービス端末１２が、複数のサービス端末からなるネットワークの一部である場合には、サービス端末のネットワークのセンタ要素が、異なるサービス端末からの認証要求を、好ましくはこのセンタ要素とＨＬＲの間の常設接続を介して、ＨＬＲに転送するようにしてもよい。

【００２８】図２は、ステップ２１から２５までを含む、本発明による方法の実施形態を示す流れ図である。

【００２９】ステップ２１は、ハイブリッド無線端末からサービス端末へ商取引要求を送信するステップである。このステージでは、通常のブルートゥースで標準化された接続手続きを用いることができる。

【００３０】ステップ２２も、この標準化された接続手続きの一部であり、サービスステーションにおいてハイブリッド無線端末の識別を実行するステップである。この識別には、各ブルートゥース対応デバイスを同定する固有の４８ビットアドレスが使用される。

【００３１】ステップ２３は、本発明に従って、ステッ

プ２２で実行されるデバイス識別に加えて、ユーザ認証を実行するステップである。このステージでは、ハイブリッド無線端末の識別モジュールに記憶された認証情報は、ブルートゥースのインタフェースを介して特有のメッセージでサービス端末に伝送される。このユーザ認証情報は、ハイブリッド無線端末が通信可能な無線通信ネットワーク内でのユーザ認証にも使うのが好ましい。

【００３２】ステップ２４は、この特定のメッセージをサービス端末で受け取り次第、ユーザ認証情報の抽出を行うとともに、サービス端末を用いてセキュリティの確保された商取引を実行することを許可されたすべてのユーザのユーザ認証情報を包含するデータベースとの照合を実行するステップである。

【００３３】認証が正常に終了した場合、すなわちそのユーザが、そのサービス端末でセキュリティを確保された商取引の実行を許可されたユーザの一人である場合には、サービス端末は、ハイブリッド無線端末に肯定応答を送信してユーザからの商取引要求を承認する。

【００３４】ステップ２５は、商取引そのものを実行するステップである。

【００３５】ステップ２４での認証が正常に終了しなかった場合は、商取引要求は拒否される。追加のセキュリティ機構として、この不成功商取引に関するパラメータをログファイルに記憶し、不審な商取引行為を検出してもよい。

【００３６】好ましい一実施形態においては、傍受行動を防止するために、ユーザ認証情報を含むメッセージを暗号化によって保護してもよい。これは、保護されていないユーザ認証情報を傍受することで、悪意を持つ傍受者がユーザ名を使って金銭取引を実行できるので、特に重要である。暗号化メカニズムとしては、当業者に通常知られている任意のものが考えられる。ハイブリッド無線端末の通信可能な無線通信ネットワークで使われているものと同じ暗号化メカニズムを使用することができる。

【００３７】図３は本発明によるハイブリッド無線端末の一実施形態を示す。ハイブリッド無線端末３０は、２つのパート３１と３２を備える。第１のパート３１は、例えばＧＳＭやUMTＳのような一般の無線通信ネットワークとの通信のサポート専用である。

【００３８】第１パート３１は、アンテナ３１１、無線通信ネットワークとのインタフェース、第１の送／受信モジュール３１２、第１の通信コントローラ３１３、および加入者識別モジュール３１４を備える。

【００３９】第２パート３２は、無線インタフェースを介してサービス端末と通信するための近距離無線インタフェース３２１、第２の送／受信モジュール３２２、および第２の通信コントローラ３２３を備える。このインタフェースに用いる標準は、ブルートゥースが好ましい。

【００４０】従来技術による解決策においては、この種のハイブリッド端末の２つのパート３１と３２は、互いに独立している。これとは反対に、本発明によれば、加入者識別モジュール３１４は、第１パート３１と第２パート３２によって共有されており、第２通信コントローラ３２３は、このモジュールからユーザ認証情報を抽出するために、加入者識別モジュール３１４にアクセスして、それを適当なメッセージにして、送／受信モジュール３２２と近距離無線インタフェース上のインタフェース３２１とを介して伝送することができる。

【００４１】ハイブリッド無線端末３０の他の実施形態においては、２つの送／受信装置３１２と３２２、または２つの通信コントローラ３１３と３２３を、物理的に同一実体上に配置して、通信プロセスが２つのパートを区別して制御するようにしてもよい。その場合には、第２パート３２の通信を制御するプロセスが、加入者識別モジュール３１４へのアクセス権を有することになり、このことも本発明の範囲に入るものである。

【００４２】図４は、本発明によるサービス端末の一実施形態を示す。サービス端末４０は、近距離無線インタフェース４１、送／受信モジュール４２、通信コントローラ４３、認証モジュール４４、および認証データベース４５を備える。

【００４３】インタフェース４１と送／受信装置４２を介してメッセージを受信すると、このメッセージは通信コントローラ４３に転送され、前記通信コントローラは、このメッセージがユーザ認証情報を含む認証メッセージかどうかを検出する。そうである場合には、このメッセージは認証モジュール４４に転送され、認証モジュールは、ユーザ認証情報とデータベース内容とを照合するように認証データベース４５に要求する。

【００４４】前述したように、認証データベースは、サービス端末の外部にあってもよい。この場合には、認証モジュール４４は、専用のインタフェースを介して、この外部データベースに認証要求を送信する。

【００４５】さらに前述したように、ユーザ認証情報は暗号化してもよい。ユーザ認証情報を暗号解読して、データベース内容と照合するのも、認証モジュールのタスクである。認証が正常に終了した場合は、認証モジュール４４は通信コントローラをトリガして、送／受信装置４２とインタフェース４１を介して商取引の承認を送信する。

【００４６】結論として、本発明によれば、通常の無線通信ネットワークと近距離無線通信システムの間でユーザ認証情報を共有することで、ハイブリッド無線端末のユーザにとって新たな付加価値があり、かつセキュリティが確保された用途が生み出される。

【図面の簡単な説明】

【図１】本発明による方法を実施可能なシステムを示す図である。

9　　10

【図２】本発明による方法の一実施形態を示す流れ図である。

【図３】本発明による無線端末の一実施形態を示す図である。

【図４】本発明によるサービス端末の一実施形態を示す図である。

【符号の説明】

１１、３０　ハイブリッド無線端末

１２、４０　サービス端末

１３　基地局

１４　無線通信ネットワーク

１５、４５　認証データベース

３１　無線端末の第１パート

＊３２　無線端末の第２パート

４１、１１２、３２１　近距離無線インタフェース

４２　送／受信装置

４３　通信コントローラ

４４　認証モジュール

１１１　アンテナ

１１２　近距離無線インタフェース

３１２　第１送／受信モジュール

３１３　第１通信コントローラ

３１４　ユーザ認証モジュール、加入者識別モジュール

３２１　近距離無線インタフェース

３２２　第２送／受信モジュール

３２３　第２通信コントローラ

【図１】

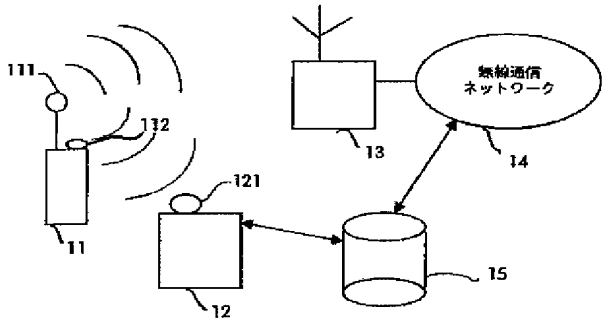

Fig 1

【図２】

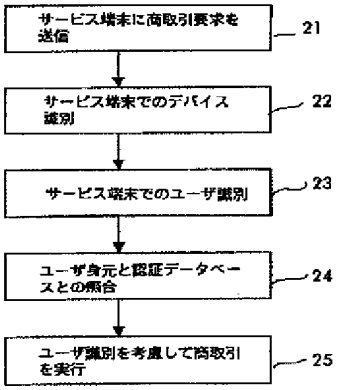

Fig 2

【図３】

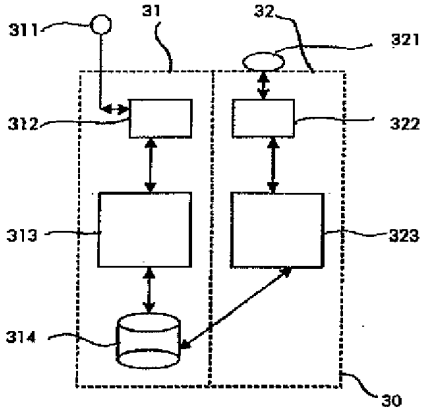

Fig 3

【図４】

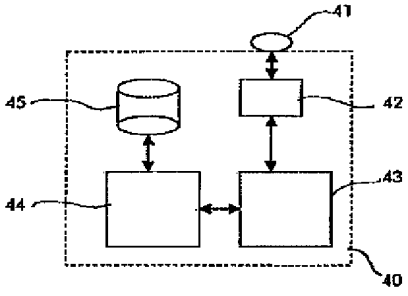

Fig 4

フロントページの続き

Ｆターム(参考)　5K067 AA30 AA32 BB04 DD17 EE02
EE16 EE35 FF02 HH23 HH36
KK15

50

【外国語明細書】

1. Title of Invention

A METHOD FOR PERFORMING SHORT-RANGE WIRELESS TRANSACTIONS BETWEEN AN HYBRID WIRELESS TERMINAL AND A SERVICE TERMINAL OVER AN INTERFACE FOR SHORT-RANGE WIRELESS ACCESS AND CORRESPONDING SERVICE TERMINAL.

2. Claims

1/ Method for performing a short-range wireless transaction between an hybrid wireless terminal (11, 30) and a service terminal (12), said hybrid terminal (11) being able to communicate over a first interface (111) with a radio communication network (14) and over a second interface for short-range wireless access (112) with said service terminal (12), said hybrid wireless terminal (11) comprising a user authentication information for authenticating a user in said radio communication network (14), said method being characterized in that it comprises the steps of:

- transmitting over said second interface (112) a message to said service terminal (12) comprising said user authentication information;
- authenticating said user at said service terminal (12) by checking said received user authentication information against an authentication database (15);
- enabling said transaction if said user authentication has been successful.

2/ Method according to claim 1, characterized in that said authentication database (15) is shared by said service terminal (12) and said radio communication network (14).

3/ Method according to claim 2, characterized in that said authentication database (15) is the Home Location Register (HLR) of said radio communication network (14).

4/ Method according to any of the claims 1 to 3, characterized in that said interface for short-range access at said hybrid wireless terminal (11) and at said service terminal (12) are compliant with the Bluetooth standard.

5/ Method to any of the claims 1 to 4, characterized in that said user authentication information is part of a SIM (Subscriber Identity Module) card.

6/ Service terminal (40) dedicated to perform a transaction over a short-range wireless interface (41), characterized in that it comprises:

- means (42, 43) for receiving a user authentication information from a wireless terminal, said user authentication information being dedicated to authenticate a user in a radio communication network;
- an authentication module (44) for authenticating said user at said service terminal (40) by checking said received user authentication information against an authentication database (45) of said radio communication network, said authentication module enabling said transaction if said authentication has been successful.

7/ Service terminal (40) according to claim 6 characterized in that it further comprises decryption means for decrypting said received user authentication information according to a predefined decryption algorithm.

8/ Wireless terminal (11, 30) comprising a first part (31) for communicating with a radio communication network and a second part (32) for communicating with a service terminal over a short-range wireless interface

(321), said first part (31) comprising a user authentication module (314) for authenticating a user in said radio communication network, said wireless terminal (30) being characterized in that said second part (32) has access to said user authentication module (314) and transmits at least an user authentication information contained in said user authentication module (314) over said short-range wireless access interface (321) to said service terminal for authenticating said user in said service terminal.

9/ Wireless terminal (11, 30) according to claim 8, characterized in that it further performs encryption of said user authentication information according to a predefined encryption algorithm before transmitting said user authentication information over said short-range wireless interface.

3. Detailed Description of Invention

The present invention relates to wireless short-range data communication systems and more particularly to a method for performing short-range wireless transactions between an hybrid wireless terminal and a service terminal.

An hybrid wireless terminal should be understood as a wireless terminal dedicated to access to a radio communication network, as for example a GSM mobile phone or third generation UMTS mobile phone, further comprising an interface for short-range wireless access, for example a Bluetooth interface. An example of such an hybrid wireless terminal is already known from Bluetooth Specification Version 1.0 B page 100 from 1 December 1999 and describes the "3-in-1 phone" model with built-in Bluetooth technology.

At home, the "3-in 1 phone" functions as a cordless telephone. On the move, it functions as a cellular telephone. For these two first applications, the mobile telephone uses the usual interface to a radio communication network at home the 3-in-1 phone communicates for example over DECT to a local base station, on the moves, the 3-in-1 phone communicates over GSM.

In a third configuration, when the 3-in-1 phone comes within the range of another mobile phone with built-in Bluetooth technology, it functions as a walkie-talkie and communicates exclusively with the other mobile phone over the Bluetooth interface. In that case the communication does not require resources from a radio communication network. Moreover, the communication is not billed.

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, personal digital assistants and other stand-alone devices can easily interconnect with each other using a short-range wireless connection. The technology requires that a low-cost transceiver chip be included in each device. Each device is equipped with a microchip transceiver that transmits and receives in a frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). The maximum range between two Bluetooth equipped devices for setting up a connection is 10 meters. Data as well as voice communications can be set up over the Bluetooth interface. Data can be exchanged at a rate of 1 megabits per second (up to 2 Mbps in the second generation of the technology). A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. Each device is identified by a unique 48-bit address defined in the Bluetooth standard. Built-in encryption and verification of this unique address is provided for ensuring the connection security. However, the verification described in the Bluetooth standard is uniquely based on a device identification. This identification prevents a Bluetooh device not registered at another Bluetooth device to communicate with it. A drawback of this device-based identification is that no user authentication is possible and as a consequence a lot of applications requiring a user authentication are not possible over the short-range wireless Bluetooth interface.

The term service terminal is used to cover terminals that are able to provide a service to a user that starts a transaction with this service terminal over a short range wireless interface. During a transaction, a user requests a service to be provided by the service terminal, the transaction comprises a dialog between the user and the service terminal for checking the modalities in which the service has to be provided as well as an authentication of the

user. If the authentication has been successful, the service terminal provides the service to the user and ends the transaction.

Since the services provided by the service terminal are preferably billed to the user, the authentication of the user is required for authorizing the service terminal provider to be credited the amount of money required for the service. Possible examples of service terminals entering this category are: a toll gate that opens automatically and deducts the toll gate price from the bank account of drivers equipped with an hybrid mobile phone with Bluetooth interface, a drink automate that is controlled by an hybrid mobile phone from a user wanting to buy a drink, the cost of this drink being deducted from his bank account or added to his phone bill.

On the other hand, the services provided by a service terminal may be confidential. In that case, an authentication of the user is also required to preserve confidentiality. Example of service terminals entering this category are printers of bank account extracts controlled with an hybrid mobile phone or printers of medical reports controlled over an hybrid mobile phone.

A particular object of the present invention is to provide a method enlarging the spectrum of applications supported by an hybrid mobile phone in providing a method for user authentication over the short-range wireless interface.

Another object of the invention is to take advantage of the capabilities of an hybrid terminal to reduce the load produced by certain applications on the radio communication network.

These objects, and others that appear below, are achieved by a method for performing a short-range wireless transaction between an hybrid wireless terminal and a service terminal, the hybrid terminal being able to communicate over a first interface with radio communication network and over a second interface for short-range wireless access with a

service terminal, the hybrid wireless terminal comprising a user authentication information for authenticating a user in the radio communication network. The method consists in performing the steps of:

- transmitting over the second interface for short-range wireless access a message to the service terminal comprising at least the user authentication information;
- authenticating the user at the service terminal by checking the received user authentication information against an authentication database;
- enabling the transaction if the user authentication has been successful.

This method has the advantage that a transaction between the hybrid wireless terminal and the service terminal is independent on the radio communication network coverage. Indeed, even if the user is located in an area where no radio communication network coverage is provided, he can make a transaction with the service terminal.

Another advantage of this method is that a transaction with the service terminal and a communication over the radio communication network can be performed simultaneously since the transaction with the service terminal does not require any radio communication network resources.

The present invention also concerns a service terminal according to claim 6 and an hybrid wireless terminal according to claim 8.

Other characteristics and advantages of the invention will appear on reading the following description of a preferred implementation given by way of non-limiting illustrations, and from the accompanying drawings.

Figure 1 shows a system where a method according to the invention can be implemented. The system comprises an hybrid wireless terminal 11, a base station 13 belonging to a radio communication network 14, a service terminal 12 and an authentication database 15.

Hybrid wireless terminal 11 comprises an antenna 111 for communicating over the air interface with base station 13 of the radio communication network 14 and a short-range wireless interface 112 for communicating over the air interface with service terminal 12.

Radio communication network 14 is preferably a GSM network or an UMTS network. However, any other radio communication network providing features ensuring communication security like authentication and authorization could also be examples for radio communication network 17.

The short-range wireless interface used for communicating between hybrid wireless terminal 11 and service terminal 12 is preferably based on the Bluetooth standard. However, any other standardized short-range wireless interface may also be envisaged. Another example could be the Home RF standard. Both Bluetooth and Home RF are based on radio frequency communication. Also optical communication using infrared may be used over the short-range wireless interface. Standards defined by the Infrared Data Association (IrDa) describes such an Infrared communication.

An advantage of radio frequency communication over the short-range wireless interface is that the antenna may be used for communication with radio communication network 14 as well as with service terminal 14.

By using infrared communication on short-range wireless interface an infrared emitter should be incorporated to the hybrid terminal.

A condition for a communication to be established over the short-range wireless interface is that the distance between the hybrid wireless terminal and the service terminal is compatible with the distance indicated in the standard (i.e. up to 10 meters for Bluetooth) for the radio wave to be received properly.

Such a distance condition is usually not set for communicating with radio communication network 14 since it is the purpose of a radio communication network provider to design his network so that a whole area coverage is ensured. This is achieved by an appropriate positioning of the bases stations and the provision of hand-over procedure. The goal of short-range wireless communication, on the contrary, is to enable a communication between two devices either close to each other or even in front of each other without any obstacles in between.

According to the invention hybrid wireless terminal 11 transmits over short-range wireless interface 112 a user authentication information used at service terminal 12 to perform user authentication. This user authentication information is located in an identification module at wireless terminal 11 already dedicated to be used for authenticating the user of wireless terminal 11 in radio communication network 14. This identification module is preferably the SIM (Subscriber Identification Module) card and comprises user authentication information. Example of such user authentication information may be the IMSI or TMSI (International resp. Temporary Mobile Subscriber Identification). Other possible user authentication information enabling it to univocally identify the user may also be saved on the SIM card for example a bank account number or a PIN number.

For providing such short-range communications with security somewhat comparable to the security provided in radio communication network 14, service terminal 12 is connected to a database 15 containing user authentication information of users authorized to make transactions with service terminal 12.

This database may be physically connected to service terminal 12. Database 15 may also be part of service terminal 12 itself. In such a case, each service terminal is connected to a replicated version of database 15.

Alternatively, this database 15 may be a central element to which service terminal 12 is connected over an appropriate network. In this configuration, several service terminals may be simultaneously connected to database 15. In this case, the database contents have not to be replicated and as a consequence are less subject to data inconsistencies.

In a preferred embodiment, database 15 is the same database as the one used by the radio communication network 14 for performing authentication in the radio communication network 14. In this embodiment, database 15 may correspond to the Home Location Register (HLR) of the radio communication network 14. The service terminal 12 is allowed by the radio communication network operator to have access to the HLR over a specific secured connection. In case service terminal 12 is part of a network of a plurality of service terminals, a central entity in the network of service terminal may be responsible for forwarding the authentication requests from the different service terminals to the HLR preferably over a permanent connection between this central entity and the HLR.

Figure 2 shows a flow diagram of an embodiment of the method according to the present invention comprising steps 21 to 25.

Step 21 consists in sending a transaction request from the hybrid wireless terminal to a service terminal. At this stage, the usual Bluetooth standardized connection procedure can be used.

Step 22, also part of this standardized connection procedure, consists in performing the identification of the hybrid wireless terminal at the service station. This identification makes use of the unique 48-bit address identifying each Bluetooth capable device.

Step 23, according to the invention and additionally to the device identification performed at step 22, consists in performing user authentication. At this stage, a user authentication information stored in a identification module at the hybrid wireless terminal is transmitted in a specific message to the service terminal over the Bluetooth interface. This user authentication information is preferably also used for authenticating the user in the radio communication network, the hybrid wireless terminal is able to communicate with.

Step 24 consists, upon reception of this specific message at the service terminal, in extracting the user authentication information and performing a check against a database containing user authentication information of all users authorized to perform a secured transaction with the service terminal.

If the authentication is successful, that is to say the user is one of the users authorized to perform secured transactions with the service terminal, the service terminal sends an acknowledgement to the hybrid wireless terminal acknowledging his transaction request.

Step 25 consists in performing the transaction itself.

If the authentication at step 24 has not been successful, the transaction request is rejected. As additional security mechanism, the parameters of this unsuccessful transactions may be stored in a log file used for detecting suspicious transactions attempts.

In a preferred embodiment, the message containing the user authentication information may be protected by encryption for preventing possible interception attempts. This is all the more important as interception

of an unprotected user authentication information could enable an ill-intentioned interceptor to perform money transactions on the behalf of the user. Any usual encryption mechanisms as known by those skilled in the art may be envisaged. It is possible to use the same encryption mechanism as the one used in the radio communication network, the hybrid wireless terminal is able to communicate with.

Figure 3 shows an embodiment of an hybrid wireless terminal according to the present invention. Hybrid wireless terminal 30 comprises two parts 31 and 32. First part 31 is dedicated to support communication with a usual radio communication network as GSM or UMTS for example.

First part 31 comprises an antenna 311, interface to the radio communication network, a first sender/receiver module 312, a first communication controller 313, and a subscriber identification module 314.

Second part 32 comprises a short-range wireless interface 321 for communicating over the air interface with a service terminal, a second sender/receiver module 322 and a second communication controller 323. The standard used over this interface is preferably Bluetooth.

In prior art solutions, the two parts 31 and 32 of this kind of hybrid terminal are independent form each other. On the contrary, according to the present invention, the subscriber identification module 314 is shared by first part 31 and second part 32 so that the second communication controller 322 can access to the subscriber identification module 314 for extracting a user authentication information form this module and transmitting it in an appropriate message over sender/receiver module 322 and interface 321 on the short-range wireless interface.

In another embodiment of hybrid wireless terminal 30, the two sender/receivers 312 and 322 or the two communication controllers 313 and 323 may be located on the same physical entity, the communication process controlling the two parts being distinct. In that case the process

controlling the communication of second part 32 has access to subscriber identification module 314 what would still be in the scope of this invention.

Figure 4 shows an embodiment of a service terminal according to the present invention. Service terminal 40 comprises a short-range wireless interface 41, a sender/receiver module 42, a communication controller 43, an authentication module 44 and an authentication database 45.

When receiving an message over interface 41, and sender/receiver 42, this message is forwarded to communication controller 43, said communication controller detects if this message is an authentication message comprising a user authentication information. If it is the case, this message is forwarded to authentication module 44 which makes a request to an authentication database 45 to check the user authentication information against the database contents.

As already mentioned above, the authentication database may be external to the service terminal. In such a case, authentication module 44 sends a authentication request to this external database over a dedicated interface.

As also mentioned above, the user authentication information may be encrypted. It is also the task of the authentication module to decrypt the user authentication information before checking it against the database contents. If the authentication has been successful, the authentication module 44 triggers the communication controller to send a transaction acknowledgement over the sender/receiver 42 and the interface 41.

As a conclusion, according to this invention, sharing user authentication information between usual radio communication network and short range wireless communication system is a source of new value added and secured applications for user of hybrid wireless terminals.

4. Brief Description of Drawings

- Figure 1 shows a system where a method according to the invention can be implemented.
- Figure 2 shows a flow diagram of an embodiment of the method according to the present invention.
- Figure 3 shows an embodiment of a wireless terminal according to the present invention.
- Figure 4 shows an embodiment of a service terminal according to the present invention.

Fig. 1

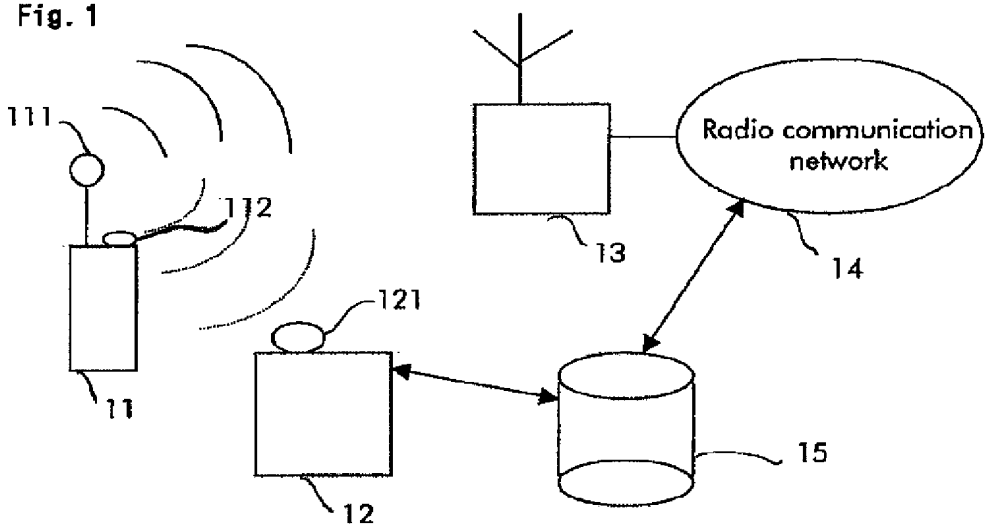

Fig 1

Fig. 2

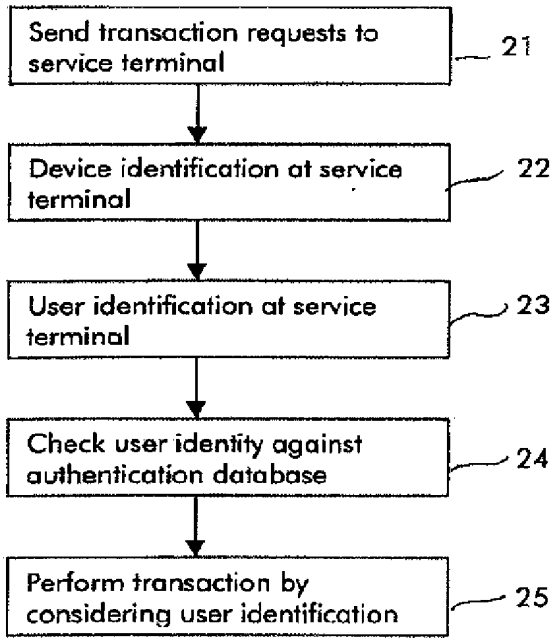

Fig 2

Fig. 3

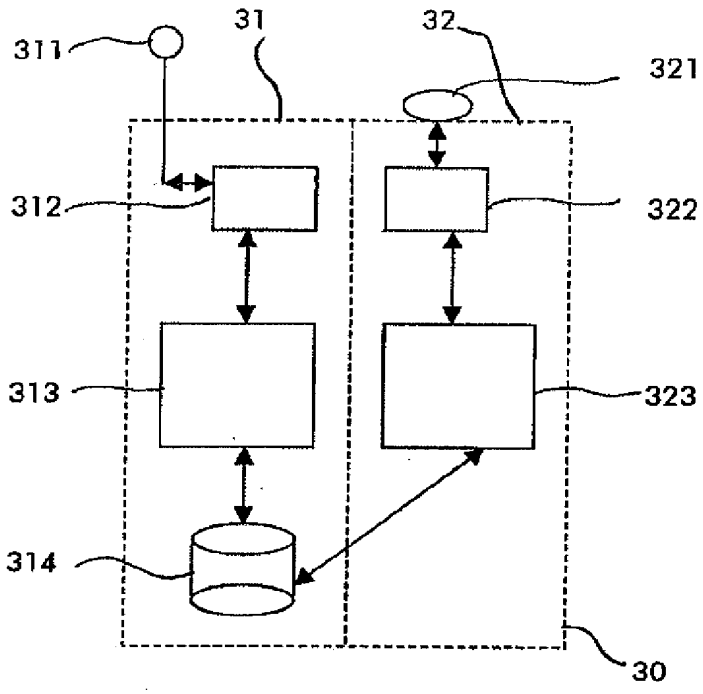

Fig 3

Fig. 4

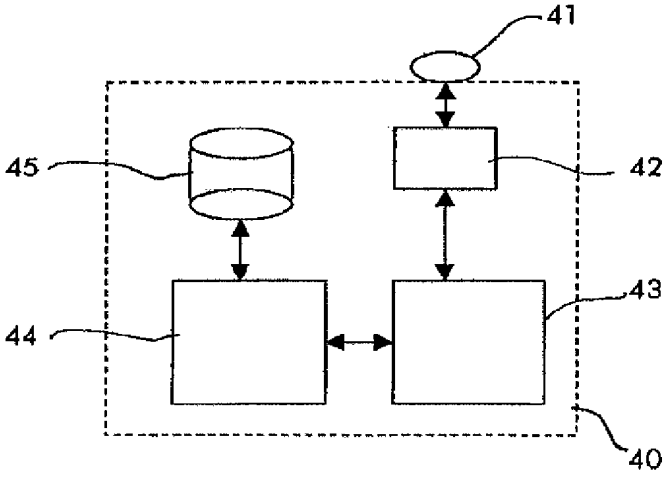

Fig 4

1. Abstract

The invention relates notably to a method for performing a short-range wireless transaction between an hybrid wireless terminal and a service terminal. The hybrid terminal is able to communicate over a first interface with a radio communication network and over a second interface for short-range wireless access with a service terminal, the hybrid wireless terminal comprises a user authentication information for authenticating a user in the radio communication network.

According to the invention, the method consists in:

- transmitting over the second interface for short-range wireless a message to the service terminal comprising at least the user authentication information;
- authenticating the user at the service terminal by checking the received user authentication information against an authentication database;
- enabling the transaction if the user authentication has been successful.

2. Representative Drawing

Fig. 1